

**A MATRIX SAFETY FRAME
APPROACH TO ROBOT SAFETY
FOR SPACE APPLICATIONS**

NABW-1333

By:

**T.D. Montgomery
L.K. Lauderbaugh**

**Department of Electrical, Computer and Systems Engineering
Department of Mechanical Engineering, Aeronautical
Engineering & Mechanics
Rensselaer Polytechnic Institute
Troy, New York 12180-3590**

December 1988

CIRSSE Document #14

CONTENTS

| | Page |
|---|------|
| LIST OF FIGURES..... | iv |
| ACKNOWLEDGEMENT..... | v |
| ABSTRACT..... | vi |
| 1. INTRODUCTION AND HISTORICAL REVIEW..... | 1 |
| 2. TERRESTRIAL ROBOTS | 8 |
| 2.1 Fatalities..... | 8 |
| 2.1.1 Identification of Common Points..... | 9 |
| 2.2 Accidents..... | 10 |
| 2.2.1 A Swedish Study | 11 |
| 2.2.2 A Japanese Study..... | 12 |
| 2.2.3 Identification of Common Points..... | 12 |
| 2.3 Robot Safety Standards..... | 14 |
| 3. SAFEGUARDING TERRESTRIAL AND SPACE ROBOTS..... | 17 |
| 3.1 Intrinsic Safety..... | 17 |
| 3.1.1 Intrinsic Design: Protecting Against Human- Robot Contact..... | 18 |
| 3.1.2 Intrinsic Design: Reliability..... | 22 |
| 3.1.3 Intrinsic Design: Kinetic Energy Control..... | 23 |
| 3.1.4 Intrinsic Operation: Robot Programming (Teaching)..... | 24 |
| 3.1.5 Intrinsic Operation: Training and Retraining..... | 27 |
| 3.2 Add-On Safety Systems..... | 28 |
| 4. SPACE ROBOTS..... | 30 |
| 4.1 Safeguarding: Environmental Concerns..... | 30 |
| 4.2 NASA Operational Modes | 31 |
| 4.3 Safeguarding: Protecting Against Astronaut-Robot Contact..... | 34 |
| 4.4 Hazard Identification Checklist..... | 36 |
| 4.4.1 Environment..... | 39 |
| 4.4.2 Mechanical Design..... | 39 |
| 4.4.3 Standard Engineering Design Practices..... | 41 |

| | | |
|--------|---------------------------------------|----|
| 4.4.4 | Gripper Design..... | 42 |
| 4.4.5 | Electrical Design..... | 42 |
| 4.4.6 | Power Supply | 43 |
| 4.4.7 | Emergency Stop..... | 43 |
| 4.4.8 | Presence Detecting | 44 |
| 4.4.9 | Control System | 44 |
| 4.4.10 | Memory Storage | 46 |
| 4.4.11 | Programming | 46 |
| 4.4.12 | Robot Location..... | 47 |
| 4.4.13 | System Layout..... | 47 |
| 4.4.14 | Robot Operations..... | 48 |
| 4.4.15 | Astronaut Training/Certification..... | 49 |
| 5. | DISCUSSION AND CONCLUSIONS..... | 51 |
| 6. | LITERATURE CITED | 53 |

LIST OF FIGURES

| | Page |
|---|------|
| Figure 1.1 Matrix Safety Frame | 4 |
| Figure 1.2 Example: One Cube of Volume in the Space Robot Matrix Safety Frame | 5 |
| Figure 4.1 Example: Two Cubes of Volume in the Space Robot Matrix Safety Frame | 38 |

ACKNOWLEDGEMENT

Many people helped me during the course of this research. The support and encouragement of Dr. Ken Lauderbaugh made it possible for this work to begin and to progress to the present stage. Without his support, this thesis and the associated degree would remain a dream. I thank Dr. Lauderbaugh for believing in me before I could believe in myself.

I wish to express gratitude also to the fellowship of my many friends for helping me through personally difficult times as well as academically difficult times. Appreciation is also given to my fellow graduate students, especially Nan, and to my office mates: Jay, Vin, Dave, Jeff, Ed and Vic for keeping life alive and interesting, and not allowing me to take myself too seriously.

Finally and most importantly, I give thanks to my Higher Power, God, for giving me life, and for guiding me to use my given talents one day at a time.

This thesis is dedicated to my mother, Amelia Stewart, for her unyielding love.

ABSTRACT

The planned use of autonomous robots in space applications has generated many new safety problems. This thesis assesses safety of autonomous robot systems through the structure of a proposed three-dimensional matrix safety frame. By identifying the common points of accidents and fatalities involving terrestrial robots, reviewing terrestrial robot safety standards and modifying and extending these results to space applications, hazards are identified and their associated risks assessed. Three components of the safeguarding dimension of the matrix safety frame, safeguarding through design and operation for intrinsic safety and incorporation of add-on safety systems, are explained through examples for both terrestrial and space robots. A space robot hazard identification checklist, a qualitative tool for robot systems designers, is developed using the structure imparted by the matrix safety frame. The development of an expert system from the contents of the checklist is discussed.

PART 1

INTRODUCTION AND HISTORICAL REVIEW

As the number of robots operating in terrestrial manufacturing facilities has increased over the past few years, so has interest in employing robots in space. Robots have relieved workers of dangerous and tedious duties, improved product quality, and cut manufacturing costs. Robots can be highly autonomous, their positioning can be extremely accurate, and their operation tireless. Robots are not, however, immune to failure. They are involved in accidents which injure people and damage equipment. In fact, terrestrial operation of autonomous robots, with their unfamiliar and often unpredictable movements and extended range of motion, has resulted in the creation of new safety hazards to add to the long list of risks associated with the operation of traditional industrial machines.

The need for safeguards has become prevalent and sources have and continue to come forward to meet this need, the result being the generation of a large quantity of suggestions for the safe design and operation of terrestrial robots. This thesis attempts to satisfy the need for structure in the study of robot safety, and applies this structure to the study of space robot safety. What was once a disjoint collection of very valuable safeguarding

information is now clearly and concisely presented in a hazard identification checklist structured around a matrix safety frame.

The current state of the art in ensuring the safety of terrestrial robots and robot systems is checklists, flow charts and fault-tree analyses. Research detailed in this thesis provides the groundwork for advancing the state of the art of robot safety, specifically for robots operating in space, to further develop the current qualitative measures by viewing robot safety in a matrix frame. In addition, research is currently underway to add quantitative measures by expanding the work presented here to develop an expert system for safe design and operation of space robots and robot systems.

A review of studies of terrestrial robot fatalities and accidents and of domestic and international robot safety standards shows the need for identifying hazards and assessing risks associated with each mode of robot system operation. Requirements for safeguarding personnel from injury and equipment from damage, a primary concern for all engineers and scientists involved with the design of robots and robot systems, can be identified by viewing robot operation in the proposed matrix safety frame. The result of this modular approach to safeguarding is a collection of recommendations for the safe design and operation of robots and robot systems. After modifying, adding and

deleting recommendations as required for operation in the space environment, the recommendations are incorporated into a hazard identification checklist, a qualitative safety tool for robot systems designers and robot users. Entries in this checklist fill discrete volumes of the matrix safety frame.

It is essential that a systematic assessment using a matrix safety frame be made of possible hazards and associated risks in individual component and systems designs, and that approaches to safeguarding be coordinated. Effort has been taken throughout this thesis to clearly identify the hazard-risk-safeguard relation. While developing safeguards to eliminate, reduce or work around each of the potential injury or damage conditions, designers must remember that safeguarding should improve the overall safety of robot system operations, and not cause the creation of secondary hazards through the safeguarding of primary hazards. For example, posts should not be used to limit a robot's range of movement because they create pinning points. The matrix safety frame will help robot system designers identify such conflicting safeguards.

A matrix safety frame for safeguarding robot systems is multi-dimensional; the three dimensions of the proposed matrix are shown in Figure 1.1: Matrix Safety Frame. The first dimension of the matrix, Dimension "M" (mode of operation), includes four modes of robot operation: Installation, Programming (Teaching),

Normal, and Maintenance (Troubleshooting). The three components of the second dimension of the matrix, dimension "S" (safeguarding), are Intrinsic Safety in Design, Intrinsic Safety in Operation, and Add-On Safety Systems. These three

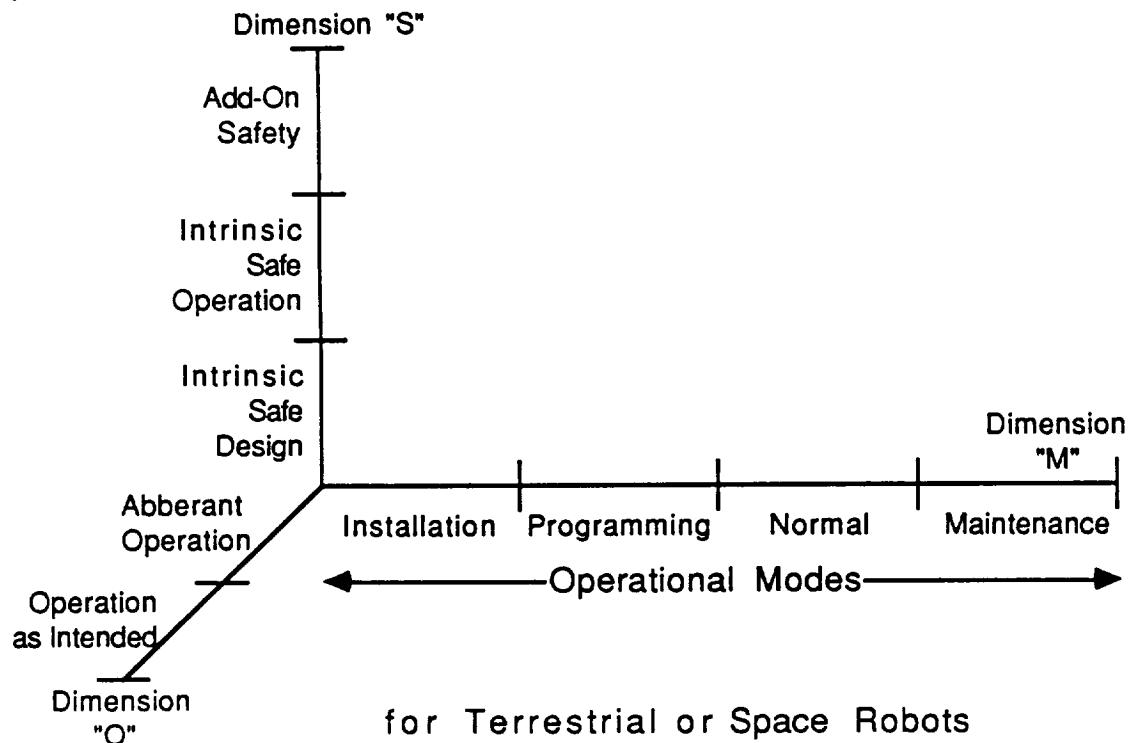


Figure 1.1 Matrix Safety Frame

components are discussed in detail for both terrestrial and space robots in Parts 3 and 4. Dimension three, referred to as "O" (operation), has two components, Operation as Intended, and Aberrant Operation occurring as a result of one or more failures. This three-dimensional matrix safety frame exists for robots operated in both the terrestrial and space environments. The

proposed frame can easily be fitted to any robot installation by modifying the components of the dimensions and/or adding new dimensions.

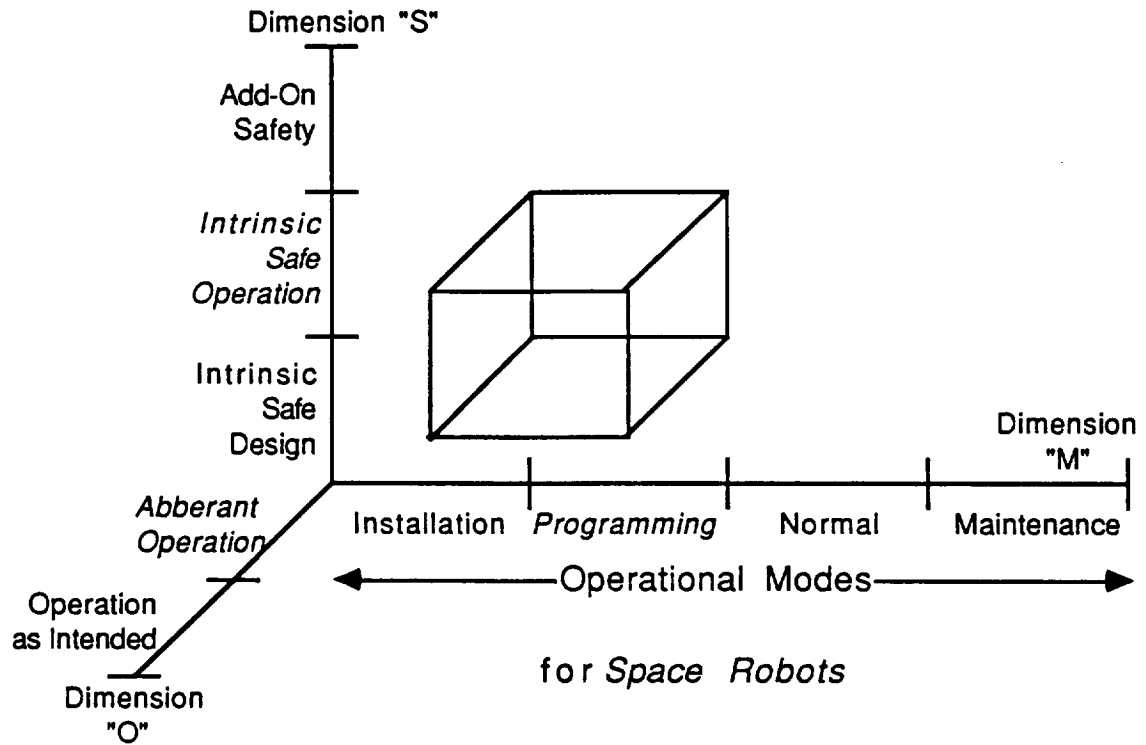


Figure 1.2 Example: Space Robot Matrix Safety Frame

Example: Intrinsic Safe Operation of Space Robot under Abberant Operation during Programming

The modular nature of safeguarding using a matrix safety frame can be seen through an examination of Figure 1.2 Example: Space Robot Matrix Safety Frame. Through inspection we can count a total of $4 \times 3 \times 2 = 24$ cubes in the three-dimensional frame. These are the cubes of volume which we will isolate when using

the hazard identification checklist to assess safeguarding requirements . The example displayed in the figure is intrinsic safety in the operation (dimension S) of a space robot for aberrant operation under a subsystems failure (dimension O) during programming (teaching) (dimension M). We see that this example fills one cube of volume in the complete three-dimensional matrix safety frame.

The hazard assessment for a robot system is the summation of individual investigations of the injury or damage possible as a result of the dangers present in each cube of the matrix for the appropriate environment, terrestrial or space. While the given example is for one cube of volume only, a hazard assessment will typically include the volume of more than one cube. An example is given in Part 4.4

It is easy to see that a thorough hazard assessment using a matrix safety frame could be exhaustive and potentially prohibitive given time, money or other constraints, thus a quantitative or qualitative injury or damage potential could be assigned to aid in prioritization of individual hazard assessments. This prioritization could be based on an assigned level of severity of the possible human injury or equipment damage. Individual volumes of the matrix safety frame with high severity ratings could then be

assessed first, and the implementation of required safeguards be given higher priority.

Having discussed the modular approach to safeguarding using the proposed matrix safety frame, we now show the motivation for this investigation of robot safety through a review of the studies of fatalities and accidents which occur during robot operation.

PART 2

TERRESTRIAL ROBOTS

2.1 Fatalities

Despite their high operating speeds and often unpredictable movement, the total number of fatalities associated with the operation of robots is much less than with other industrial machines. In July 1983, Altamuro detailed four reported and documented Japanese fatalities associated with the operation of industrial robots (1). The fifth and most recent international fatality occurred in the United States and was detailed by the National Institute for Safety and Health (2). The higher incidence of fatalities in Japan may be attributed to their broader definition (3) of the term robot (the Japanese refer to many more classes of industrial equipment as "robotic" than we do in the United States) and to their more lengthy experience with industrial robots.

A brief review of the circumstances surrounding each of the five fatalities provides insight into hazard identification, risk assessment and safeguarding requirements.

1. Japan, July 1981. A repairman climbed a safety fence to perform maintenance in a robot's work space while the robot was in normal operation. The robot pushed him from the rear into a grinding machine and he died.

2. Japan. A worker climbed onto a moving conveyor while a robot was idle, but still operating. The robot moved and squeezed him to death.
3. Japan. A worker reactivated a robot after servicing a machine near it. The robot moved, pinning and crushing the worker to death against the machine.
4. Japan. One worker started a robot while another worker was in the robot's work space. The robot pushed the second worker into a positioning fixture and killed him.
5. US, July 1984. A worker passed through a gap in a fence surrounding an operating robot, and was pinned between the robot's arm and a safety pole. Although stalled, the robot continued to apply pressure, and crushed the worker. He died 5 days later. A legal suit was filed and his family was awarded 10 million dollars.

2.1.1 Identification of Common Points

Four common points to the natures of these fatal accidents are:

- In almost all cases, the worker entered the robot's work zone to correct a minor problem in interfacing equipment like conveyors or metal working machines, but not in the robot itself.

- While in each case the worker was trained and experienced in robot operations, he did not follow safety procedures, was complacent, took unnecessary risks, or was in error.
- The robot struck the worker from behind without warning.
- The worker was pinned between the robot and a peripheral machine or a structure in the work space, and the worker was killed by the machine or by crushing.

Hazards and associated risks are identified from the review of fatalities, and from this list of common points in fatalities, needs for safeguarding procedures become apparent. For example, it is clear from the last common point that to prevent pinning (hazard) and the resulting human injury or death (risk), a robot's work space needs to be designed to permit clearance for operators to move safely between the robot and other equipment (safeguard).

2.2 Accidents

As with our discussion of fatalities, common points can be drawn from the studies of accidents, and requirements for safeguards can be identified. Although no sources from within the United States were identified, a few sources from outside the United States were found which presented the results of studies of robot accidents. The following sections summarize the findings of accident studies conducted in Sweden and Japan, and identify their common points.

2.2.1 A Swedish Study

The report of a study (4) conducted in Sweden from 1979 through 1983 summarized 36 reported robot accidents. In almost all cases the robot was a manually controlled manipulator type, where the manipulator was performing pick and place operations.

One finding from the Swedish study was that most contact occurred during adjustment in the course of operation (14 cases) or during repair, programming, etc (13 cases). This agrees with other studies showing that of the four principal modes of operation: installation, programming (teaching), normal, and maintenance (troubleshooting), programming and maintenance are the most hazardous modes, during which the largest chance for human injury and equipment damage exists. This is because it is often necessary for a worker to be within the operational envelope of a active robot during programming and maintenance.

When a worker is in an active robot's work cell and the robot makes an unexpected movement, the worker is in danger of being struck. The possible causes of unexpected movement include, but are not limited to software error, control problems, component failure, dirty servo valves, electrical noise, frayed electrical cable, short circuits, loose connections, power surges or pressure drops, broken hydraulic or pneumatic lines, oil pressure valve

trouble, encoder and other sensor related problems, excessive heat and electronic malfunction. In addition, human errors like accidentally or prematurely returning a robot to power on position while a worker is in the robot's work cell, cause many injuries.

The Swedish study reported injuries to the following parts of the body; the number in parentheses representing the total occurrence: finger (12), hand (7), arm (2), back (4), head (6), neck (1), leg (2), rib (1), tooth (1). Most workers required only short periods of sick leave. There were no fatalities.

2.2.2 A Japanese Study

A Japanese study (5) of robot accidents found that over thirty eight percent of reported accident situations were the result of erroneous actions of robot operators. When the design of a robot is not intrinsically safe, the safe operation of the robot depends more heavily upon the skills of the person working with the robot, and the risks associated with operation are increased. This risk assessment makes clear the importance of designing intrinsically safe robots and the importance of training and continually retraining the people who work with robots.

2.2.3 Identification of Common Points

Hazards and their associated risks are easily identified in the common points of the Swedish, Japanese and other reports (6)

which detail human injuries from terrestrial robot accidents. Four common points are:

- The majority of injured workers are operators or maintenance personnel; however, the curious and risk taking outsider may make unauthorized entry into the robot's work space.
- Robot gripper to human hand contact is most typical.
- Workers are sometimes trapped or pinned by the robot against peripheral equipment or the work space enclosure.
- A robot end effector may release an object during normal or aberrant operation, or during a stop, and that object may contact and injure a worker.

Another important hazard to recognize is that a robot may appear "dead" when in fact, it is powered and is in a software dictated hold period, waiting for its next move command. A worker could interpret this inactive status as powered down and approach the robot, placing himself in danger of physical injury (risk). To safeguard against this hazard, it is recommended that rotating lights be positioned on the top on robots to indicate a power on condition. A rotating light indicator is fail safe, since failure of both the bulb and of the rotating mechanism are required for indicator failure. This is yet another example of how the identification of hazards allows for the assessment of risks and the determination of safeguarding requirements. The next section

discusses the standardization of general practices for safeguarding terrestrial robots and robot systems.

2.3 Robot Safety Standards

Because of a robot's operational characteristics, including its wide range of programmable movements, and its unique nature of association with operators and maintenance personnel, safeguarding standards for traditional industrial machines and equipment are not completely applicable to robots and robot systems. Discussions of the necessity for and the development of safety standards for industrial robots and robot systems were contained in many reports and articles (5,7,8,9,10,11).

A number of countries have developed specialized standards for robot safety; names of domestic and international standards and comments about the standards (where available) are (12):

USA

ANSI/RIA 15.06-1986, "American National Standard for Industrial Robots and Robot Systems - Safety Requirements.", Robotic Industries Association, 1986. The objective of the standard is to enhance the safety of personnel who work with industrial robot systems by establishing guidelines for the construction, installation, care and use of industrial robots. Compliance with this standard is voluntary. The standard specifically excludes space robots.

- UK Machine Tools Trade Association (MTTA),
"Safeguarding Industrial Robots, Part 1: Basic Principles.", 1982. MTTA, with Health and Safety Executive (HSA) assistance, developed a industry code of practice covering hazard identification, risk assessment and safeguarding of industrial robots, with emphasis on programming and maintenance modes.
- USSR GOST-SSBT, "Industrial Robots, Robotised Installations and Robotised Shops.", 1982.
- Japan JIS B 8433, "General Code of Safety for Industrial Robots.", 1983.
- West Germany VDI Guideline 2853, "Safety Requirements Relating to the Construction, Equipment and Operation of Industrial Robots and Associated Devices.", 1984.
- East Germany TGL 30267/01, "Industrial Robots for Machine Tools; Terms; Requirements, Safety Measures.", 1982.
- France AFNOR Standard, in preparation.

Having presented the common points of robot fatalities and accidents, and discussed standards development, we now turn to safeguarding terrestrial and space robots and robot systems. To provide structure for the study of robot safety, we concentrate discussion around each of the three elements of the "S" dimension

of the matrix safety frame: intrinsic safety in robot system design,
intrinsic safety in robot system operation, and add-on safety
systems.

PART 3

SAFEGUARDING TERRESTRIAL AND SPACE ROBOTS

3.1 Intrinsic Safety

The best way to ensure safe operation of a robot system is to design the system for intrinsic safety. The Merriam-Webster Dictionary defines "intrinsic" as "belonging to the essential nature or constitution of a thing". An intrinsically safe system is therefore a system which has safety features inherent in the design, and which operates safely independent of external safety systems. When we recall that robots are operated by humans whose errors cause a significant percentage of industrial accidents, we see that to realize intrinsically safe operation, we must begin with intrinsically safe designs.

Much of the current literature addresses safeguarding through design and operation for intrinsic robot safety (13,14,15,16,17). One approach shared by Barrett (18) and Bellino (19) was the formulation of checklists comprising a lists of general questions which alert robot system designers to specific safety issues, and thereby help the designers improve the intrinsic safety of their systems. Components of these checklists are included in the hazard identification checklist presented later in this thesis. Other approaches to the evaluation of risks and hazards in robot design and operation were presented by Barrett, Bell and Hodson (20) in

the form of a logical analysis flow chart and by Sugimoto and Kawaguchi (3) in the form of a fault-tree analysis.

The following few sections discuss safety issues characteristic of specific areas of robot system design and operation. While most design and operating procedures are applicable to both the terrestrial and space environments, some schemes are domain limited; effort has been made to identify these situations when they are not immediately obvious.

3.1.1 Intrinsic Design: Protecting Against Human-Robot Contact

Experience has shown that it is necessary to have layers of protection between the robot and humans who share the robot's work region. The outermost layer is a peripheral barrier. If the peripheral barrier is penetrated, presence sensing capabilities are required to alert the robot system to an invasion and to initiate appropriate responses to avoid collision. Appropriate responses depend on the nature of the invasion, and include system emergency stop, system slow down and alternate end effector path planning.

The outer layer of protection for a worker from a terrestrial robot is to employ peripheral barriers like fences, ropes and chains to prevent the worker from gaining access to the operating robot's cell. In addition, the work cell may be delineated with lines painted on the floor or signs hung in the area. The most effective barrier

for preventing unauthorized access is an electrically charged interlock fence (obviously impossible in space). Through control circuitry, the power to the robot is interrupted when an interlock fence is opened, and power can not be restored until the gates are secured and an operator activates restart controls positioned outside of the peripheral barrier.

Curious or complacent workers may penetrate a peripheral barrier and enter an active robot's work cell. In order to safeguard these workers against accidents, it is necessary to equip the robot with an intelligent means of detecting people and preventing contact.

The inner layer of safeguarding against human-robot contact is the application of presence detecting devices which are linked with the robot's safety system. While the simplest form of presence detection is a pressurized floor mat which causes an emergency stop of robot activity when stepped upon, it is often necessary to employ more sophisticated tactile, proximity and range, and machine vision devices for presence detecting (21,22,23,24,25). Sophisticated sensors can detect not only a human's presence, but also an object entering the working envelope, or objects within the envelope changing positions. Kilmer (24) identifies three general types of security intrusion detection systems by the region which they cover:

- point, spot or object
- perimeter or penetration
- area, space or volumetric.

Many sensors and sensory systems are commercially available for terrestrial applications; some of these systems may be operable in the space environment. Some sensor devices are:

- light curtains/photoelectric sensors (photoreceptor and infrared directional light source)
- ultrasonic (echo-ranging), microwave, infrared, capacitance motion sensors
- magnetic field detectors
- acoustic sensors
- laser
- hall effect
- electrostatic
- vibration sensors
- supersonic
- visual
- inductive
- sonar

Each of these sensing devices has specific capabilities, ranges of operation, and reliability. By incorporating more than one type of sensor into a sensory system, that is, by utilizing multiple sensor integration (MSI), the overall safety level of the robot system can improve. Sensory information from more than one source is combined and compared to give more accurate information in real time, thus the impact of a single sensor's failure is reduced.

There are many features to consider when selecting sensors and sensory systems to operate in real time. It is recommended that sensors have the following properties:

- high accuracy
- high precision
- quick speed
- fast response
- compatibility with other components
- compatibility with the environment in which they operate
- operating range broad enough to encompass all possible hazards, but not too broad so as to take in extraneous information which would delay processing
- easy to calibrate and hard to work out of calibration
- high reliability with large mean times between component failures
- straightforward operation, with minimum room for misunderstanding or improper operation
- simple and easily understandable output characteristics (for both system operators and interfacing equipment)

Bellino (19) recommends that to improve the overall safety of a robot system through optimized performance and reliability of hardware components, the components selected should be:

- hard to bypass
- simple to use
- fail safe
- non-fragile
- easy to install and repair
- cost effective
- reliable and highly immune to false triggering

- hardened against electrical noise and industrial ambients.

A safety monitoring and control system (26) which uses presence detecting devices was developed by Harless and Donath for times when a worker must share an active robot's work cell, for example, during programming and maintenance, when complete shut down may be impractical or undesirable. At these times one of the following robot actions suggested by Henkel (27) may be more appropriate:

- slow down
- visual or audible alarm activation
- selection of an alternate path which avoids contact
- redirection of robot activity to an intruder free area.

3.1.2 Intrinsic Design: Reliability

Each component of a robot system must be designed with concern for component and system reliability. Whether fabricated in-house or procured, all components should be designed and manufactured to assure reliability. Following a formal preventative maintenance and replacement schedule is essential to the reduction of equipment failures and to the safe operation of the system. By incorporating modular component designs, replacement of components can be made straightforward to require a minimum of down-time.

3.1.3 Intrinsic Design: Kinetic Energy Control

Industrial accidents involving robots have been classified as energy-conversion accidents, where the stored energy of the robot system is mischanneled into a form which injures people or equipment (3). In order to minimize the injury and/or damage which accompanies a collision, it is important to design robot components to dissipate stored energy. This is particularly necessary during periods of emergency power reduction.

High levels of kinetic energy are especially dangerous in collisions, and control gets more complex and less reliable as the level of kinetic energy increases. There are a number of ways to reduce kinetic energy levels. Although the obvious approach is to limit speed, it is equally important to design the robot arms to minimize inertia. Arm material, mass distribution and geometric shape must all be considered. Kinetic energy absorption through the use of mechanical stops, shock absorbers, damping within the drive system and dynamic or frictional braking can also be incorporated into the design of robot systems, or the kinetic energy could be converted to elastic energy of spring type components.

Electrical, thermal, radioactive and high pressure energy sources should also be identified and safe release of those energies incorporated into the robot system's design. Leipold advises that stored energy devices like pneumatic accumulators, springs and

capacitors need locking systems or stored energy release methods, and that all connections be designed to prevent mismatching and inadvertent disconnection (16).

Having discussed three areas of design for intrinsic safety of robot systems: protecting against human-robot contact, reliability and kinetic energy control, we now view operation for intrinsic safety through discussions of robot programming and operator training and retraining.

3.1.4 Intrinsic Operation: Robot Programming (Teaching)

Programming a robot to perform a series of actions is referred to as teaching. As was already mentioned, programming is one of the most hazardous modes of robot operation because it is often necessary for the teacher to be within the working envelope of the operating robot. Possible risks of injury to a worker include being:

- struck by the robot
- struck by an object which the robot gripper releases
- contacted by material used in the application (ex: paint spray)
- pinned by the robot arm against the work space enclosure or peripheral equipment.

Risks of damage to equipment in the enclosure, the enclosure itself, the robot, or the robot's work piece also exist.

A number of safeguards are available to eliminate or minimize these risks. The first three recommendations for intrinsically safe operation are not specific to the programming (teaching) mode. Note that many of these points correspond also to intrinsically safe design requirements, and therefore include more than one cube in the matrix safety frame.

- People should not be present in the robot's work envelope during initial start-up or during restart after hardware or software modification, repair or relocation, until proper operation of the system is verified.
- All emergency stops must be functional.
- Restart of the robot after emergency shut-down should be possible only from outside the robot's work cell and only after all systems have returned to normal operation. Restart should require a minimum of two operations, not simply resetting of the switch which caused the shut-down.
- Restart should not be initiated from a teach pendent.
- When a robot is in the teach mode, whether it is controlled through a mobile teach pendent or the main console, the robot should operate at a reduced velocity; this reduced velocity will ensure that the forces and torques present do not present hazards if human/robot contact should occur.

Although it is difficult to generalize from one robot system to the next, a maximum velocity of 250 mm/sec has been suggested by many sources, including the American National

Standard. (In space this maximum velocity will need to be lower.)

- Teachers should be thoroughly trained and certified to perform programming using both a teach pendant and the main console.
- The internal control circuitry should ensure that the teacher have complete control of the robot and any peripheral equipment which may present a hazard while s/he is within the restricted work envelope. The main robot controller should not produce robot or peripheral equipment motion.
- Control of the robot by two or more teachers should be avoided.
- All motion causing control devices (buttons, switches, etc.) on the teach pendant must be continuously activated to sustain motion.
- The teach pendant should have a three position deadman switch which initiates an emergency stop if the handle is either released or squeezed too tightly, as it may be in an emergency or panic situation.
 - This switch should be deadwired to the stop circuit, and not pass through software links, which when down, could fail to prevent an emergency stop.
 - There should be separate drive and encoder disconnects, so that when the robot is powered down in an emergency stop situation, position data is not lost.

Because it is important to match safeguards with the people performing the activity in which the hazard is present, we now focus attention on the training, certification and retraining of personnel who work with robot systems.

3.1.5 Intrinsic Operation: Training and Retraining

The strongest means of safeguarding against human injury is through training and retraining the personnel who interact with the robot system. To reduce worker's contributions to accidents, they must be skilled in robot operation and safety procedures. Initial training must be rigorous and thorough and should follow training documents which are easily understood and readily referenced in either hard copy form or on-line at a computer terminal. Periodic retraining is essential to refresh the worker's memory and to prevent the worker from either risk taking or becoming complacent. Personnel who will not have authorized access should be trained to realize the risks involved with robot operations and the necessity to remain outside of the robot's work space. Injury to the curious or complacent bystander can be prevented through education.

3.2 Add-On Safety Systems

Having completed a discussion of intrinsic safety, it is important that we recognize the distinction between safe design and operation "internal" to a robot system and safety achieved through the incorporation of systems "external" to the robot system (add-on safety systems). For the purpose of illustration, we can see that sophisticated sensor systems like Harless and Donath's (26) which rely on the operation of the robot controller are internal to the robot system. The stand alone safety systems discussed below do not rely on the robot controller, but instead work in parallel with the robot system and are add-on safety systems by definition.

Note that principles of intrinsic design and operation for safety are equally applicable to robot systems and add-on safety systems; the reference frames of intrinsic design/intrinsic operation and robot system/add-on safety system overlap and should not be viewed as mutually exclusive.

As was mentioned previously in our discussion of intrinsic design, once a workers presence has been detected by the sensors in the inner layer of protection, the next step is collision avoidance, the simplest form of which is complete shut down of the robot. One sophisticated collision avoidance systems is a stand alone safety system developed at Rensselaer (28,29,30). This

system uses capacitance and acoustic elements and employs special mapping algorithms and dedicated processors to map and memorize features within the operating range of the robot. When defined parameters are violated during robot operation, corrective actions are taken.

A second add-on safety system, a Watchdog Safety Computer system (31), was installed in the Automated Manufacturing Research Facility at the National Bureau of Standards. This auxiliary safety computer monitors status and sensory inputs from the robot, the controller and other sources, and when position, velocity or acceleration values for any of the six joints or for the tool point exceed the maximum operator selected values, the safety computer stops the robot and notifies the system operator.

PART 4

SPACE ROBOTS

In an effort to provide structure to the study of robot safety, the discussion has thus far centered around the "S" dimension of the matrix safety frame, safeguarding for the intrinsic design and operational safety of terrestrial and space robots and robot systems and for the inclusion of add-on safety systems. At this point, we focus attention primarily on space robots and robot systems by discussing intrinsic safety and add-on safety issues specific to space applications of robots. Drawing together the information contained throughout this thesis and viewing it in the matrix safety frame, we then formulate a hazard identification checklist of questions for space systems designers to answer to assess the safety of robot systems and system components. Research continues to develop an expert system from the expanded contents of this checklist.

4.1 Safeguarding: Environmental Concerns

Terrestrial robots typically operate in a very well defined and predictable environment, where the environmental conditions usually do not vary widely; conversely, space robots will operate in the dynamic space environment, where the world model is continually changing, and the robot system itself is highly

autonomous. Operation in this environment presents numberable design challenges. For example, many of the sensors available today may not be able to meet the demands of operation in space, thus we are presented with the challenge of developing sensing and computational capabilities to update the world model in real time.

When selecting all components that constitute a space robot system design, the hazards associated with exposure to and operation in the space environment must be considered. For example, designs should safeguard against damage from the most severe combination of (32):

- electromagnetic interference (EMI)
- cosmic radiation
- earth generated radio frequency noise
- penetrating charged particles (ionizing radiation)
- meteoroids and space debris
- neutral atmosphere density
- induced environment and effects
- magnetic fields
- gravitational effects
- plasma environments.

4.2 NASA Operational Modes

NASA (33) identifies four modes of operation for space robots: teleoperation, both with and without an astronaut present,

autonomous, combined teleoperation and autonomous, and transitional between teleoperation and autonomous. The programming and normal components of the "M" (Mode of Operation) dimension of the proposed matrix safety frame can easily be modified to include NASA modes.

The teleoperation of space robots poses unique safety problems. First, the state of the art in teleoperation will need to be advanced to satisfy the requirements of the space application. Further developments of the state of the art in safety systems for teleoperated robots will also be required.

In line with terrestrial recommendations, it is essential that when a space robot is being teleoperated, and an astronaut is within the working envelope of the robot, the astronaut have complete control of the robot and any peripheral equipment that could present a hazard. To support this recommendation, let us look back at the issues surrounding accidents and fatalities resulting from terrestrial robot-human contact. Recall that the greatest danger of accident or death occurs during programming and maintenance, when the worker is in closest proximity to the robot. For the worker to have anything less than complete control of the robot and peripheral equipment is very dangerous.

While it may be advisable that two astronauts work together near a space robot, dual control of the robot is very dangerous and should not be possible. One astronaut should have complete operational and shut down control, while the other astronaut has only emergency stop control. (All astronauts should have robot emergency stop control designed into their space suits.) The fourth fatal accident internationally occurred when one worker returned a robot's power before a second worker was out of the robot's work envelope and that second worker was killed.

Return to autonomous mode of operation after teleoperation should be prevented until it is verified that all astronauts are outside of the robot's work envelope. The issue of whether initiation of autonomous operation should be possible from a mobile teach pendant or only from the main console must be determined.

Recall that in the matrix safety frame, each operational mode is cross-matched with operation as intended and aberrant operation occurring as a result of one or more failure. During aberrant operation, appropriate responses to system and component failures must be preplanned and incorporated into the system design to prevent human injury and equipment damage. As a minimum requirement, all robot systems should be designed so that they may be safely powered down.

4.3 Safeguarding: Protecting Against Astronaut-Robot Contact

NASA documents point out that not all of the astronaut crew will be certified as robot operators. However, all astronauts who enter the robot's work space must be protected. One way of protecting the authorized astronaut is to ensure that he has complete robot control, but what about preventing unauthorized astronaut entry into the robot's work space? One terrestrial way of safeguarding against unauthorized entry is to put up protective barriers and lay down pressure sensitive mats. Needless to say, there must be a different approach to preventing astronaut-robot contact in the space application.

Safeguards must be available to prevent accidental contact or collision between the robot and an astronaut. The problem can be approached from two sides: How can we make an astronaut aware of the robot's position and activity? and How can we make the robot aware of the astronaut's position and activity? An industry proven way of alerting a worker to the status of a robot has been to have a visual display like a rotating light atop an activated robot. This alone is not enough of a safeguard because an astronaut could still unknowingly drift backwards into the robot, and be struck by the robot. Focus must turn to the second approach to solve the problem of preventing astronaut-robot contact.

Astronaut presence-detecting proximity sensors like those discussed in Part 3 could be incorporated into the design of the space robot system, and appropriate reaction, for example, collision avoidance through power down, speed reduction, or alternate path planning, could be programmed into the robot's operating software or safety system software. In space, we have the advantage that an astronaut will always be wearing a space suit which can be designed to include sensors and transmitters that are part of the presence sensing system. Thus, if an astronaut were to drift unknowingly into the robot's work space, the robot would be able to recognize the astronaut and react to avoid contact. To return again to the first approach, information from the presence-detecting devices could be relayed by way of an audio warning signal or a "heads up display" in the astronaut's space suit to inform her/him of the robot's status and of her/his distance from the robot. The astronaut would then be able to react to avoid the robot.

Finally, we would like to point out a fact of human nature. After people have experience in performing a task, they may become over confident or complacent, and may be tempted to shortcut safety safeguards so as to quicken or simplify a procedure. In order to protect against human erroneous actions, guards against improper astronaut use of the space robot must be designed into the robot and its operating systems.

4.4 Hazard Identification Checklist

By developing upon terrestrial experiences, checklists and flow charts and by modifying, adding and deleting items to tailor recommendations to the space environment, we formulated the following space robot hazard identification checklist using the structure provided by the matrix safety frame. The checklist is a tool for space based robot systems designers to use to identify the source of potential hazards, assess the associated risks, and design appropriate safeguards. In order to safeguard a robot system to prevent human injury and equipment damage, a hazard identification check should be made of each component and system design in each cube of volume of the matrix safety frame.

Entries in the checklist are identified with codes for the volume of space in the matrix safety frame which is covered. The codes used in the checklist are as follows:

| <u>Code-Dimension-Component</u> | | <u>Code-Dimension-Component</u> | |
|---------------------------------|--------------|---------------------------------|----------------|
| M:I Mode | Installation | S:D Safeguard | Intrinsic Safe |
| Design | | | |
| M:P Mode | Programming | S:O Safeguard | Intrinsic Safe |
| Operation | | | |
| M:N Mode | Normal | S:A Safeguard | Add-On Safety |
| M:M Mode | Maintenance | O:A Operation | Abberant |
| | | O:I Operation | As Intended |

The checklist is written primarily for space based robots and robot systems, but most entries are applicable also for terrestrial applications.

Recall that one entry in the checklist will often correspond to more than one cube if volume in the matrix safety frame, for example, the code M:N S:A O:A,I will cover a total of two cubes, seen in the example matrix safety frame for the space environment: Figure 4.1.

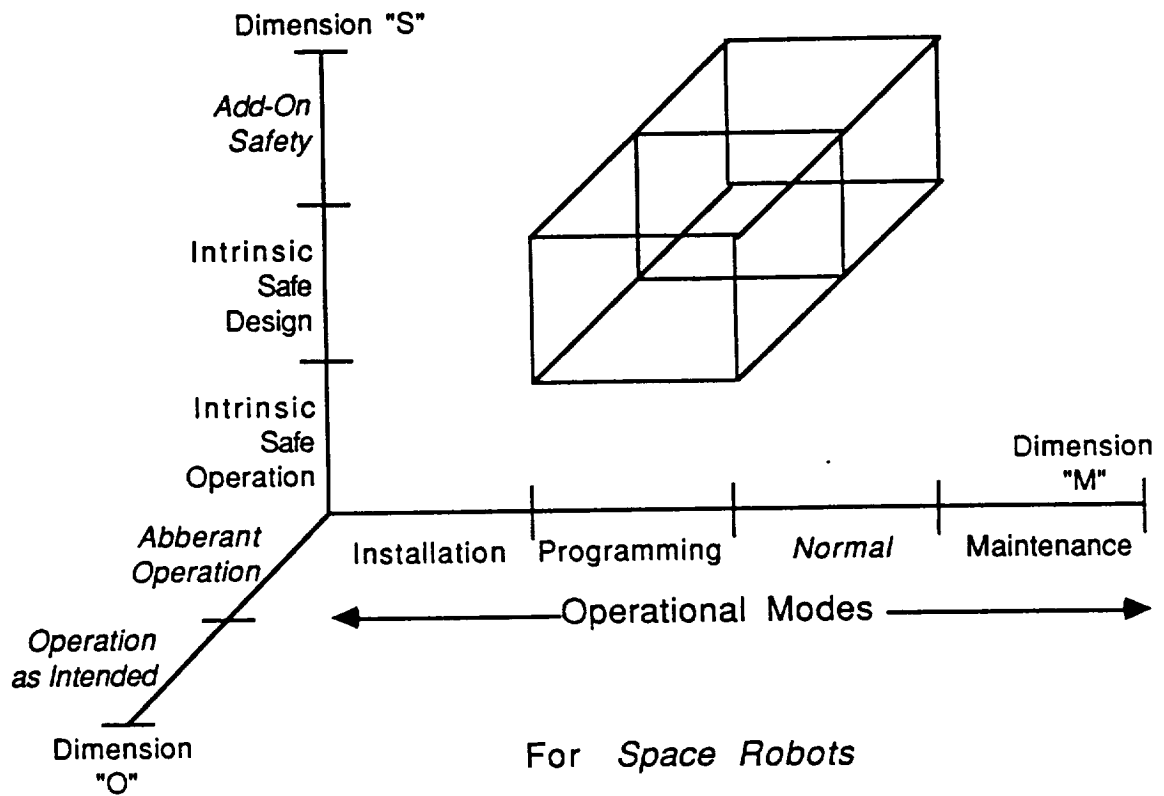


Figure 4.1
Example: 2 Cubes of Volume for
Space Robot Matrix Safety Frame

4.4.1 Environment

- (E:S M: I,P,N,M S:D,A O:A,I) Do all system designs (control system, actuators, power supplies, etc.) safeguard against damage from the most severe combinations of natural environments, including but not limited to:
 - * electromagnetic radiation fields (EMR)
 - * electro-magnetic interference (EMI) which could effect electronic controllers
 - * electrostatic effects
 - * electrical storms
 - * magnetic fields
 - * earth and space generated radio frequency interference (RFI) which could effect electronic controllers
 - * earth's gravitational effects
 - * penetrating charged particles (ionizing radiation)
 - * meteoroids and space debris (including dust)
 - * neutral atmosphere density
 - * induced environment and effects
 - * plasma environments
 - * temperature which could effect the control system

4.4.2 Mechanical Design

- (M:P,N,M S:D O:A,I) Have means of controlling vibration disturbances been incorporated into the system design?

- (M:P,N,M S:O O:A,I) What is the safe range of speed of movement for the grippers during each operational mode, including teaching/programming, normal and maintenance/troubleshooting (each with and without an astronaut present)?
- (M:P,N,M S:D O:A,I) Are the robot arms able to withstand the forces and torques associated with the maximum possible working loads at the maximum possible speeds?
- (M:P,N,M S:D O:A,I) Are shear pins or breakaway sections designed in the equipment to ensure robot failure occur before pinning and crushing forces are reached?
- (M:P,N,M S:D O:A,I) Are physical restraints like chains, pins and bolt-ons located at the extremes of robot movement able to withstand maximum operating forces and torques?
- (M:P,N,M S:D O:A,I) Are hardware stops and brakes strong enough to stop the robot arms when they are moving at their top speeds and carrying their maximum loads?
- (M:P,N,M S:D O:A,I) Are hardware stops and brakes operational even during power failures?
- (M:P,N,M S:A O:A,I) Could cushion padding cover the robot at points where impact with an astronaut is most likely?
- (M:P,N,M S:D O:A,I) Does the system contain stored energy which could cause damage to the robot, other equipment or an astronaut if inadvertently released? Has safe release of all of the following energies been designed into the system?
 - * kinetic energy associated with robot motion

- * high pressure energy in ruptureable fluid lines (pneumatic)
- * electrical energy which could result in electric shock
- * chemical or biological energy from sources in area
- * thermal energy from radiation
- * radioactivity
- (M:I S:A O:I) Is the robot adequately protected when installed and in storage?

4.4.3 Standard Engineering Design Practices

- (M:I,P,N,M S:D O:A,I) Are components and subsystems designed to comply with applicable recognized codes, regulations and safety standards? (ex: ANSI/NFPA 79-1985, Electrical Standard for Industrial Machinery)
- (M:I,P,N,M S:D O:A,I) Is the robot's exterior free of protrusions which may cause snagging or tearing of an astronaut's space suit?
- (M:I,P,N,M S:D O:A,I) Are all sharp edges and corners covered or eliminated? (especially important on the grippers)
- (M:I,P,N,M S:D O:A,I) Do guards cover drive mechanisms, gears and pinch points?
- (M:P,N,M S:D O:A,I) Have all hoses and cables in which an astronaut or equipment could become entangled been secured or routed internal? (this will also prevent swelling in the event of a ruptured line or broken connection)

- (M:P,N,M S:D O:A,I) Are electrical cables protected from excessive wear during arm movement to prevent fraying and possible short-circuiting or shocking?
- (M:I,P,N,M S:D,O O:A,I) All all cable connections secure?
- (M:P,N,M S:D O:A,I) Have standard engineering design practices been followed in all of the robot subsystems, including the mechanical, electrical, electronic, sensory, control and safety systems?

4.4.4 Gripper Design

- (M:P,N,M S:D O:A,I) Have the end effectors been designed "fail-safe" by using more than one gripping mechanism?
- (M:P,N,M S:D O:A,I) To prevent accidental release of material into space, are robot grippers designed to retain tools or work pieces when in a state of emergency stop or power loss?
- (M:P,N,M S:A O:A,I) If gripper release during power loss can not be assured, would tethering be possible?

4.4.5 Electrical Design

- (M:P,N,M S:D O:A,I) Are there fail safe features to guard against short circuits and other failures?
- (M:P,N,M S:D O:A,I) Do the electronics have guards against contact bounce?
- (M:P,N,M S:D O:A,I) Are there separate encoder and drive disconnects to preserve position memory in the event of drive disconnect (emergency stop)?

4.4.6 Power Supply

- (M:P,N,M S:D O:A,I) Are there means to prevent conducted interferences on the main power supplies?
- (M:P,N,M S:D O:A,I) Have sensors been included to monitor and control the power supply to the robot so as to prevent power surges and large time drifts (volts/cycle)?
- (M:P,N,M S:D O:A,I) Are the power supplies adequately filtered to prevent damage in the event of power surges?
- (M:P,N,M S:D O:A) How does power loss or interruption effect the system?
- (M:P,N,M S:D O:A,I) When the speed of movement is varied, is it through primary power source reduction as opposed to control circuitry? (This will ensure a faster response unaffected by software or control failures.)

4.4.7 Emergency Stop

- (M:P,N,M S:O O:A,I) Are emergency stop switches readily accessible in and out of the robot's work cell?
- (M:P,N,M S:D O:I) Are emergency stop switches incorporated into the design of astronaut space suits?
- (M:P,N,M S:D O:I) Are emergency stop switches hardware based components and not controller based?
- (M:P,N,M S:D O:A,I) Do emergency stops override all other robot controls from all sources (control panel, teach pendants)?

- (M:P,N,M S:D O:A,I) Are emergency stops hardwired to interrupt the power supply to the robot drives, disengage clutches, activate brakes and cause all motion to cease?
- (M:P,N,M S:D O:A,I) Is the teach pendent power control a deadman switch which must be depressed to activate and which when released causes motion to stop? Is it a three position deadman's switch which also causes motion to stop if it is squeezed too tight, as it may be in a crisis situation?

4.4.8 Presence Detecting

- (M:P,N,M S:D,A O:A,I) Can the robot system and/or an add-on safety system detect an astronaut in the robot's work envelope?
- (M:P,N,M S:D O:A,I) Will the robot power down or slow down to prevent human/robot collision if the system detects an unauthorized astronaut in its work envelope?
- (M:P,N,M S:D O:I) If power down is desired when an astronaut enters the robot's work envelope, have all intrusion detectors been wired in series with emergency stop circuits?
- (M:P,N,M S:D O:A,I) Is it possible for the robot to avoid a collision with an astronaut through path planning?

4.4.9 Control System

Note: The following require that the logic system be active and that the robot be calibrated correctly

- (M:P,N,M S:D O:A) Has an assessment been made of the consequences of failure of the robot control elements?

- (M:P,N,M S:D O:A,I) Are arm speed and position, and time to execute monitored and controlled to ensure safe operation?
- (M:P,N,M S:D O:A,I) Are the limits of arm speed and the travel limit enforced for each servo control drive to ensure safe operation?
- (M:P,N,M S:D O:A,I) Is the robot's maximum speed during the teaching/programming, normal and troubleshooting/maintenance modes of operation imposed to ensure safe operation?
- (M:P,N,M S:D O:A,I) Have appropriate responses to the following interrupts been programmed?
 - * excessive following error on each servo control drive
 - * abnormal velocity or acceleration on each servo control drive
 - * hardware travel limits
 - * abnormal temperature, voltage, current sensors
 - * communication data flow abnormalities
 - * shut down signals from outside interfaces
- (M:P,N,M S:D O:A,I) Are there checks on the condition and function of control components for self diagnosis and prediction of performance deterioration?
- (M:P,N,M S:D O:A,I) Can the robot system detect system or component malfunctions and notify the operational or control system as required?
- (M:P,N,M S:D O:A,I) Can the robot system monitor and regulate process conditions, pneumatic pressure for example?

4.4.10 Memory Storage

- (M:P,N,M S:D O:A,I) Is the main memory storage nonvolatile to prevent loss of data during operation?
- (M:P,N,M S:D O:A,I) Are programs held in memory in a form which prevents loss or corruption of data during information transfer?
- (M:P,N,M S:D O:A) What is the effect of data loss during program loading?
- (M:P,N,M S:D O:A,I) Is memory protected during planned and unexpected power loss?
- (M:P,N,M S:D O:A,I) If more than one program is held in memory at any time, can security between programs be ensured to prevent overwriting existing programs with data and to prevent execution of jumps between blocks of memory?
- (M:P,N,M S:D O:A,I) Are specific safety interlocks which improve the safety of the system contained in the software?

4.4.11 Programming

- (M:P,N,M S:O O:I) Is preformed by the robot manufacturer and by the robot user consistent?
- (M:P,N,M S:D,O O:A,I) How is program editing done? During reprogramming, can existing data be lost or altered?
- (M:P,N,M S:O O:A,I) Is program security ensured to prevent programming by unauthorized astronauts?
- (M:P,N,M S:O O:I) Is software operation clearly and efficiently documented and are the documents readily available to users in both hard copy and on-line at a computer terminal?

- (M:P,N,M S:O O:I) Is software user-friendly and easily operated?
- (M:P,N,M S:D,O O:I) Can programming be performed from a mobile teach pendant in addition to the main console? If so, is the teach pendant layout ergonomically designed? Are controls clearly identified and appropriately spaced to avoid inadvertent operation? Are motion causing controls designed to operate only when continuously activated?

4.4.12 Robot Location

- (M:I S:D O:A,I) Is the robot securely positioned at its work site to prevent accidental release or movement?
- (M:I S:D O:A,I) Is adequate clearance between the robot and the space station structure and other equipment assured to prevent contact and the pinning an astronaut?

4.4.13 System Layout

- (M:I S:O O:I) Is the main control console located outside of the robot's work envelope but within direct sight of the robot?
- (M:I S:O O:I) Have the proper interfaces with remote material handling equipment been included?
- (M:P,N,M S:O O:A,I) Are interfaces with peripheral equipment operational?
- (M:P,N,M S:O O:A,I) Are add-on safety systems operational?
- (M:P,N,M S:D O:A,I) Are the modular components and subsystems designed so that they are compatible with existing interfaces?

Are their designs flexible enough to be compatible with future modules?

- (M:P,N,M S:D O:A,I) What are the available diagnostic facilities?
- (M:P,N,M S:D O:A,I) What are the possible consequences of system malfunctions?
- (M:P,N,M S:O O:A,I) Are safety backup systems operating?
- (M:P,N,M S:D O:A,I) Is the speed of response of the safety system sufficiently fast for worst case conditions?

4.4.14 Robot Operations

- (M:I,P,N,M S:D,A O:A,I) Do robot system workers wear protective clothing?
- (M:P,N,M S:O O:A,I) Can a controlled shut down process be initiated under normal and emergency conditions?
- (M:P,N,M S:O O:A,I) Are a minimum of two manual actions required prior to restart after an emergency shut down?
- (M:P,N,M S:O O:A,I) Can it be verified that all safety violations have been removed prior to a system re-start?
- (M:P,N,M S:O O:I) Does the operating system software verify that all astronauts have moved outside of the robot's work space before normal operation may resume?
- (M:P,N,M S:O O:I) Can normal operation be safely initiated by a mobile teach pendent, or must it be initiated by the main console?

- (M:P,N,M S:O O:A,I) Are operations inhibited pending the completion of other independent operations?
- (M:P,N,M S:O O:A,I) Does operation with a teach pendent automatically remove operational control from the main console?
- (M:P,N,M S:O O:A) Can a collision be prevented in the event of a software failure?
- (M:P,N,M S:O O:A) Is operation prevented if a robot joint or end effector position is out of calibration?
- (M:P,N,M S:D,O O:A) Can controls which hold the last state be overridden when an end effector has closed around an astronaut's glove or other part of his space suit?
- (M:P,N,M S:D,O O:A) Can controls which hold the last state be overridden when the robot has trapped or pinned an astronaut?
- (M:P,N,M S:O O:A,I) Can the robot be moved through an undefined pathway?
- (M:P,N,M S:O O:A,I) Have adequate controls been installed to prevent a collision of movable equipment in the event of a software failure?
- (M:P,N,M S:D O:A,I) Is program checking used during system testing and operation?

4.4.15 Astronaut Training/Certification

- (M:P,N,M S:O O:A,I) Is close interaction of the robot and astronauts required?

- (M:I,P,N,M S:O O:A,I) Which astronauts will perform specific functions like mechanical and electrical component maintenance, programming, troubleshooting, etc.?
- (M:P,N,M S:O O:A,I) Is astronaut training of robot system operation thorough?
- (M:P,N,M S:O O:A,I) Are astronauts thoroughly trained in software operation?
- (M:P,N,M S:O O:I) Is periodic retraining performed?
- (M:I,P,N,M S:O O:I) Are training documents clear and concise and available in hard copy form as well as on-line at a computer terminal?
- (M:P,N,M S:D O:A,I) Are robot activity status and position information available to all astronauts? Is an activity status a visual signal like a revolving light displayed on the robot? Do the astronauts have a "heads up" display of the robot activity status?

PART 5

DISCUSSION AND CONCLUSIONS

In an effort to motivate the study of robot safety, we presented the findings of reports of terrestrial robot accidents and fatalities and drew together common points. Having set the stage for the study, we then provided information on international safety standards development. From the early part of the investigation, it became evident that to ensure safe operation of robots and robot systems, systems must be designed for intrinsic safety.

A three-dimensional matrix safety frame was proposed as a means of providing structure to an otherwise unstructured mass of safeguarding information. By performing a hazard assessment and risk analysis for each cube of volume in the matrix safety frame for a space robot systems, we are able to identify safeguarding requirements. Specific recommendations for safe design and operation of space based robots and robot systems were presented as part of a discussion of intrinsic safety in design and operation for both the robot system and add-on safety systems. Space based robot safeguarding recommendations were then organized into the three-dimensional matrix safety frame and incorporated into a hazard identification checklist. The checklist is not all inclusive,

but instead gives us a starting point from which to extend further developments.

A point was raised that a thorough hazard assessment using a matrix safety frame could be exhaustive and potentially prohibitive given time, money or other constraints. The prospect of assigning a quantitative or qualitative injury or damage potential to aid in prioritizing individual hazard assessments will also need to be further explored.

Much work remains to be done to determine the feasibility of expanding the information presented in this thesis to develop an expert system for safe design and operation of space robots and robot systems. Once feasibility has been assured, the actual development of a frames and/or rules based expert system will require the collaboration of a team of personnel from various engineering disciplines. The goal of having the expert knowledge of senior robot system designers, operators and maintenance personnel systematically organized for interactive reference by newer, less experienced robot designers, operators and maintenance personnel remains to be realized.

PART 6

LITERATURE CITED

1. Altamuro, Vincent M., "Working Safely with the Iron Collar Worker.", National Safety News, July 1983. Reprinted: Working Safely with Industrial Robots, Strubhar, Peter M., ed., pp 73-75.
2. Courter, Eileen, "Toward Safer Robots.", Working Safely with Industrial Robots, Strubhar, Peter M., ed., pp 234-236.
3. Sugimoto, N. and Kawaguchi, K., "Fault-Tree Analysis of Hazards Created by Robots.", Proceedings of the 13th International Symposium on Industrial Robots and Robots 7, April 1983. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 83-100.
4. Carlsson, J., "Robot Accidents in Sweden.", report published by Arbetarskyddsstyrelsen, National Board of Occupational Safety and Health, Sweden, 1984. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 49-64.
5. Sugimoto, N., "Systematic Robot-Related Accidents and Standardisation of Safety Measures.", Proceedings of the 14th International Symposium on Industrial Robots, 2-4 October

- 1984, Gothenburg, Sweden. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 23-29.
6. "Study on Accidents Involving Industrial Robots.", Occupational Safety and Health Department, Tokyo, Japan, August 1983. Translation of Robotics Report No. 5, Ministry of Labor, Tokyo, February 1983, 14p.
 7. Bloodgood, John, "An Overview of Standards Development for Robots and Robot Systems.", Proceedings of The Workshop on Robot Standards, June 1985, pp 1-5.
 8. Bloodgood, John, "Survey on Robot Standards.", Proceedings of The Workshop on Robot Standards, June 1985, pp 47-57.
 9. Lauck, Kenneth E., "Development of a Robot Safety Standard.", Working Safely with Industrial Robots, Strubhar, Peter M., ed., pp 227-233.
 10. Ottinger, Lester V. and Stauffer, Robert N., "Update on Robotic Standards Development.", Robotics Today, October 1983. Reprinted: Working Safely with Industrial Robots, Strubhar, Peter M., ed., pp 237-241.
 11. Prange, James M. and Peyton, James A., "Standards Development.", Robotics Today, December 1986, pp 23-24.
 12. Percival, N., "Safety Standards in Robotics.", Robot Safety Seminar Proceedings (Univ. Nottingham/Ford Motor Co.), (updated March 1985). Reprinted: International Trends in

- Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 17-21.
13. Akeel, Hadi A., "Hardware for Robotic Safety Systems.", Tower Conference Management Company's Second Annual International Robot Conference, October 1984, pp 67-74.
 14. Akeel, Hadi A., "Intrinsic Robot Safety.", Proceedings of the Conference on Robotic Safety. Reprinted: Working Safely with Industrial Robots, Strubhar, Peter M., ed., pp 61-68.
 15. Jones, Richard and Dawson, Sandra, "The Role of Hardware, Software and People in Safeguarding Robot Production Systems.", Proceedings of the 15th International Symposium on Industrial Robots, Vol. 2, September 1985, pp 557-568.
 16. Leipold, Forrest P., "Robot Construction (Safety Considerations).", RIA Robot Safety Seminar Proceedings, 1985, pp 38-43.
 17. Linger, Matts; Sjostrom, Hasse; and Palmers, Goran, "How to Design Safety Functions in the Control System and for the Grippers of Industrial Robots.", Proceedings of the 15th International Symposium on Industrial Robots, Vol. 2, Sept 1985, pp 569-577.
 18. Barrett, R. J., "Robot Safety and the Law.", Robot Safety Seminar Proceedings, November 1982. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 127-132.

19. Bellino, J. P., "Design for Safeguarding.", RIA Robot Safety Seminar Proceedings, November 1984. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 127-132.
20. Barrett, R. J.; Bell, R.; and Hodson, P. H., "Planning for Robot Installation and Maintenance: A Safety Framework.", Proceedings 4th British Robot Association Annual Conference, 1981.
21. "Photoelectric Guarding.", Internal report prepared by Manufacturing Safety Coordination, Ford of Europe, January 1985. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds., pp 199-204.
22. "Sensors for Robot Safety.", Robotics World, May 1983, pp 16-19.
23. Irwin, Christopher T. and Caughman, Don O., "Intelligent Robotic Integrated Ultrasonic System.", Proceedings of Robots 9 Conference, Vol. 2, June 1985, pp 19-38 to 19-47.
24. Kilmer, R. D., "Safety Sensor Systems.", Proceedings of Robots VI Conference, March 1982. Reprinted: International Trends in Manufacturing Technology: Robot Safety, Bonney, M. C. and Yong, Y. F., eds, pp 223-236.
25. McArthur, Gary R., "Robot Sensors and Safety with Sensors.", Proceedings of Robots 9 Conference, Vol. 1, June 1985, pp 11-97 to 11-103.

26. Harless, Mark and Donath, Max, "An Intelligent Safety System for Unstructured Human/Robot Systems.", Proceedings of Robots 9 Conference, Vol. 2, June 1985, pp 19-9 to 19-20.
27. vL Henkel, Stephanie, "Robots and Safety: An Industry Overview.", Robotics Age, July 1985, pp 26-28.
28. Derby, Stephen J.; Graham, James H.; and Meagher, John F., "A Robot Safety and Collision Avoidance Controller.", Proceedings of the Robots 8 Conference, Vol. 2, June 1984, pp 21-33 to 21-41.
29. Graham, James H.; Meagher, John F.; and Derby, Stephen J., "A Safety and Collision Avoidance System for Industrial Robots.", IEEE Transactions on Industrial Applications, Vol. IA-22, No. 1, January/February 1986, pp 195-203.
30. Millard, Don, "Robot Safety Research at RPI: A Compilation.", June 1986. Available upon request from Rensselaer.
31. Kilmer, R. D., et al, "Watchdog Safety Computer Design and Implementation.", Proceedings of the RI/SME Robots 8 Conference, June 1984. Reprinted: Working Safely with Industrial Robots, Strubhar, Peter M., ed, pp 101-117.
32. NASA Doc JSC 30425, "Space Station Program Natural Environment Definition for Design", January 15, 1987.
33. NASA Doc SS-GSFC-0031, "Flight Telerobotic Servicer (FTS) Strawman Concept Engineering Report", March 15, 1987.